The Role of Nation State Actors

& The Risks to Australian SMEs

Table of Contents

Introduction

It's no secret that the world is divided along geopolitical borders, distinguishing states not only physically, but by ideology and objectives as well. Cybersecurity is often viewed as a battle between two opponents: cybercriminals and cyber defence. However, there is a third dimension that recent global events have once again thrust into the spotlight–the nation-state actor.

In this paper, we look at the threat of nation-state actors to Australian SMEs. With far bigger budgets, superior expertise, and a legal mandate, they are believed to be far more formidable than traditional cybercrime groups. However, their motives are very different, and their capabilities are often kept secret, so the threat they pose to local businesses can be hard to determine.

Nation-State Actors

A nation-state actor is a group that possesses cyber offensive/defensive capabilities and is directed, funded, or assisted technically by a nation-state.

They are often extremely well-funded, technologically advanced, and benefit from operating within the bounds of the law in the country of origin. Examples of nation-state actors include the USA's National Security Agency (NSA), the UK's Government Communications Headquarters (GCHQ), The Australian Secret Intelligence Service (ASIS), China's specialized military network warfare forces, North Korea's Lazarus Group and Russia's Federal Agency of Government Communications and Information (FAGCI).

Below, we detail the key differences between nation-state actors and traditional cyber threat actors: funding, legality, motives, and operational secrecy.

Funding–Nation-state actors receive their funding from national budgets, rather than generating revenue as a result of their operations. Because offensive and defensive cyber capabilities are often seen as of national importance, they receive significantly more in budgetary funding than traditional cyber threat actors can generate. The most successful global cybercrime groups are estimated to make approximately $50 million USD per year[1] . By comparison, the top funded nation-state actor, the cyber elements of the USA's Department of Defence, receives $9.6 billion USD per year[2] , which is nearly 200 times more.
Legality–Similar to branches of the armed forces, nation-state actors have a legal mandate to possess equipment and capabilities that would be illegal for private citizens and organisations. Additionally, their actions are often viewed as ethical since they're aligned with the national interest, whereas similar actions undertaken by traditional threat actors are rarely considered so.

This, along with funding differences, results in nation-state actors obtaining far superior levels of expertise, higher calibre employees, and more formidable capabilities. Traditional threat groups are limited to recruiting individuals willing to engage in illegal and unethical activities, and often must recruit via anonymous, unreliable underground forums. Nation-state actors can recruit directly from universities and head hunt highly skilled individuals from the private sector.

[1] https://www.zdnet.com/article/ransomware-gangs-made-at-least-350-million-in-2020/
[2] https://www.lawfareblog.com/cyber-budget-shows-what-us-values%E2%80%94and-it-isnt-defense

Motives–As previously stated, where most cyber threat groups operate to generate revenue for themselves, a nation-state actor's motives and objectives are aligned with those of their nation. The drive for commercial gain often results in traditional threat actors employing tactics such as data extortion and ransomware. Nation-state actors, however, are more likely to be engaged in developing offensive, destructive, and disruptive capabilities for use during wartime, activities relating to espionage, theft of intellectual property, and the spreading of propaganda or misinformation.

Additionally, while a traditional threat actor's methods may change, their motives rarely differ from the generation of profit, which makes them somewhat predictable. The motives of nation state actors, however, shift and change with the geopolitical climate. Conflict, changes in trade conditions, ruling political parties, political ideology, international relations, and foreign policy can all alter the motives of states, which will filter down and result in changing actions and capabilities of their cyber actors.

Operational secrecy–Most cyber offensive strategies are based on identifying and exploiting gaps in defensive capabilities of adversaries. If the defensive gap becomes known to the adversary, it can be easily closed, rendering the offensive approach useless. This is why nation-state actors keep their most potent capabilities secret.

Think of it this way: if two neighbours are feuding and one knows that the other has left a window unlocked, they have an advantage. However, if that information becomes public, the adversary can simply lock the window and remove the advantage. The same is true of most cyber offensive capabilities.

As a result, many activities and capabilities of nation-state actors are shrouded in the highest levels of secrecy and classified as top secret. While very little information about their exact capabilities is publicly available, we can infer based on historical events.

The World's First Cyberweapon

In 2010, a computer virus called Stuxnet was discovered, which soon became known as the world's first cyberweapon. It gained this notoriety due to its complexity and highly targeted nature. Stuxnet contained not one, but four separate zero-day vulnerabilities. In fact, it was so advanced that it was able to infect almost 10% of Windows PCs globally and went undetected for several years[3] . One major reason for this was the very specific damage it caused. Despite infecting a massive number of PCs, it only did damage to programmable logic controllers (PLCs) used within Iranian nuclear facilities. The virus would cause centrifuges to spin faster than their maximum limit, while reporting a lower speed to monitoring stations, damaging devices and impeding the nuclear enrichment process.

This is a prime example of nation-state actor activity. If a ransomware was sophisticated enough to infect almost 10% of PCs, it could generate significant income for a traditional threat actor. Instead, this virus was used very specifically to help achieve the goals of several nations.

Stuxnet was written before the first iPhone was released, and in the 15 years that have passed since its creation, traditional threat actors have yet to build anything even remotely close to its sophistication.

Unfortunately, while Stuxnet caused limited damage outside of its intended target, once discovered, the virus was modified and put to use by other groups with more nefarious purposes. While the vulnerabilities it exploited were patched, reducing its effectiveness, Stuxnet has been used by criminal groups to develop at least three other malware tools targeting legitimate businesses for profit. This demonstrates an unintended consequence of nation-state actors' significant cyber capabilities.

Although no nation-state has claimed responsibility for Stuxnet, security researchers widely believe it was created by the USA in partnership with Israel.

[3] https://docs.broadcom.com/docs/security-response-w32-stuxnet-dossier-11-en

NSA Tools Are Leaked and Turned Against Their Creators

In 2016, a traditional threat group known as The Shadow Brokers hacked into systems belonging to the NSA. They sold, and later publicly released, some of their advanced cyberweapons, which were repurposed by criminal groups and other nation-state actors for use against private businesses and allies of the United States. The toolsets contained at least 5 zero-day vulnerabilities that were previously unknown to the security community, and those are thought to have been only a tiny portion of the NSA's cyber arsenal.

Up To 18000 Victims in a Single Attack

In 2020, a cyberattack was detected which infiltrated thousands of private businesses and government organisations, in what has since become known as the most sophisticated cyberattack in history.

The attacker was able to penetrate the defence of a company called SolarWinds, which provides network monitoring software to many large enterprises. While a traditional threat actor would quickly deploy malware or ransomware to maximise the chance of making a profit before being detected, this attacker operated differently.
Once access was gained, they spent months slowly moving through SolarWinds' network, using several never-before-seen techniques. They then entered SolarWinds' software patching process, demonstrating an in-depth understanding of the business and technical environment. With incredible patience and foresight, the attacker first added only a single line of benign code to a software update, most likely to test if it would be detected. When it was not, they added highly sophisticated malware to a SolarWinds' next update, which SolarWinds themselves then distributed to all their clients.
The malware was potentially distributed to up to 18,000 clients and impacted an undisclosed number. It was later confirmed that highly secure environments such as the US National Security Agency and National Nuclear Security Administration were among those impacted.

Again, this malware could have had incredible revenue potential for cybercrime groups, but it was designed to steal intellectual property. The techniques, patience, and business acumen used in its distribution hint at an extremely sophisticated attacker.

Escalating Political Tension Results in Cyber Destruction

In 2016, hostilities between Russia and Ukraine began to escalate. At the same time, virus known as NotPetya caused global panic. While initially believed to be ransomware due to its offers of decryption for a fee, researchers later found that not a single victim had obtained a decryption key through payment, and decryption was technically impossible due to the way the malware operated. This led them to realise it was designed purely to cause disruption.

The virus was traced back to an unknown, but highly sophisticated attacker breaching a Ukrainian software business and distributing NotPetya within Ukrainian accounting software. As a result more than 80% of the victims were located within Ukraine, and while major companies such as FedEx and Merck made headlines for suffering losses of more then 300 million USD each, both companies traced the problem back to the Ukrainian accounting software installed on a single PC.

Many security researchers, along with the USA and UK governments, later attributed the attack to a Russian nation-state actor, with the White House estimating the total damage to have exceeded 10 billion USD[4] globally.

The Cycle Repeats in 2022

Similarly, just hours prior to Russia's 2022 invasion of Ukraine, massive cyberattacks in the form of malware and DDoS attacks were launched against Ukraine, taking banking and government websites offline and paving the way for disorder ahead of the physical invasion. As of March 2022, data demonstrates that Ukrainian internet users are experiencing ten times more attempted cyber-attacks than their European neighbours[5] .

Russia denied responsibility for these cyberattacks, which the USA has disputed by publicly attributing them to the GRU[67] .

Judging the full capabilities of any nation-state actor is extremely difficult; however, many security researchers liken the difference between ransomware gangs and nation-state actors to the difference between traditional organised crime groups and national armies.

While an organised crime group may possess worrying violent potential, their capability pales in comparison to a well-funded, professionally trained, and fully equipped army. Similarly, while ransomware gangs possess worrying cybercrime tools, they pale in comparison to a well-funded, well-trained nation-state actor.

[4] https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/
[5] https://krebsonsecurity.com/2022/03/report-recent-10x-increase-in-cyberattacks-on-ukraine/
[6] https://www.cnbc.com/2022/02/23/cyberattack-hits-ukrainian-banks-and-government-websites.html
[7] https://www.nytimes.com/2022/01/14/world/europe/hackers-ukraine-government-sites.html

The Risk to Australian SMEs

During late February, as tensions between Russia and Ukraine were escalating, the Australian Cyber Security Centre (ACSC) released a high-priority alert[8] to all Australian businesses. This alert was not due to any specific malware or new attack vector, but was an acknowledgement by the ACSC that nation-states with strong cyber capabilities pose greater risk to industry during times of tension. Now that Australia has joined its allies in publicly denouncing Russia's actions with sanctions against their economy, this cyber risk has further increased. The threats to Australian businesses can be placed into two categories–direct and indirect:

Direct Threats

Similar to the use of a nation-state's armed forces, the direct, targeted, and persistent application of a nation-state actor's full cyber capabilities would be devastating for any business, no matter the size.

However, also similar to the use of a nation-state's armed forces, the use of advanced cyber offensive capabilities against a business is extremely unlikely. Doing so would reveal, and thus ultimately reduce, their offensive capabilities. Instead, nation-state actors prefer to reserve these capabilities for more extreme circumstances.

Far more likely is the use of lower-level capabilities, mimicking actions of traditional threat groups. These techniques are favoured by nation-states because their source can be obfuscated and attribution of the attack, if possible, can take months. This means they can take action in response to geopolitical situations, while also publicly denying responsibility and avoiding international condemnation, similar to the NotPetya events in 2016 outlined above.

This was seen closer to home in late 2020 and early 2021, when the Chinese Communist Party's (CCP) position toward Australia shifted rapidly in response to the Australian government's comments on the origin of the Coronavirus pandemic. This filtered down to the CCP nation-state actors and Australian businesses saw a 330% increase in cyber-attacks[9] . While many experts were able to demonstrate links between the attacks and elements of the CCP, the Australian Government did not feel they had enough evidence to publicly attribute the attacks to China, and there was no official response.

These low-level untargeted nation-state attacks pose a risk to all Australian SMEs. However, the risk is similar to that of traditional threat actors.

Targeted attacks, such as those used against Ukraine in recent weeks, are unlikely to pose a problem for most Australian businesses. But with Russia's recent threat of reprisal against governments imposing sanctions on them, businesses involved in defence, critical infrastructure, and public sector supply chains should be on alert, as attackers may attempt disruption or intellectual property theft.

[8] https://www.cyber.gov.au/acsc/view-all-content/alerts/australian-organisations-encouraged-urgently-adopt-enhanced-cyber-security-posture
[9] https://www.afr.com/politics/federal/surge-in-cyber-attacks-amid-china-tensions-20200619-p554av

Indirect Threats

Far more likely to impact Australian SMEs are the indirect threats posed by nation-state actors.

The most likely indirect threat is collateral damage. Due to their vast capabilities, nation-state actors can lose control of damage done even when pursuing specific targets.

This was seen in 2017, when a virus called WannaCry escaped a North Korean development facility and infected more than 200,000 PCs in 150 different countries in less than 48 hours. This disproportionately affected medical devices such as MRI scanners and blood-storage refrigerators. Total damages to businesses around the world were estimated to exceed 4 billion USD.

The WannaCry virus was halted after less than 72 hours, when a security researcher found an inbuilt 'kill switch'. This likely existed because the cyberweapon was still in development at the time it escaped. While it's unlikely that North Korea planned to attack the health sector, the impacts were significant.

Another risk to Australian SMEs, related to nation-state actors but not caused directly by them, is attacks by cybercriminal groups sympathetic to national causes. It is well known that major ransomware strains are often designed to not infect systems which operate in the Russian language. Also, a large number online meetings for cybercriminals are conducted in Russian. This has led many to conclude that major ransomware operators are sympathetic to the Russian government.

At the onset of the Russian invasion of Ukraine, several major ransomware groups, including the prolific group behind 'Conti', declared support for the Russian cause and vowed to retaliate against any country siding with Ukraine[10] , which now includes Australia.

While these groups have performed many successful ransomware attacks against Australian SMEs in the past, and certainly pose a risk today, their declaration of support for Russia has caused internal rifts amongst their members. Following the groups declaration of support, some members announced opposing views and began taking active steps to undermine the group's activities[11] . These internal rifts are currently playing out on the global stage, and are reducing the groups overall effectiveness and risk to Australian SMEs.

The final risk to Australian businesses, and the IT industry as a whole, is the policy of nation-states on vulnerabilities. As explained previously, nation-state actors have an interest in identifying vulnerabilities that can be weaponised, and keeping this knowledge secret. If a vendor realises a vulnerability is present, a patch will be released which nullifies the effectiveness of the cyber weapon.

As such, it is common for nation-state actors and intelligence agencies to identify vulnerabilities which they do not immediately disclose to vendors. This practise was brought to the forefront recently during the Log4Shell vulnerability.

This vulnerability, widely seen as the most serious in recent memory, was first discovered by a Chinese cybersecurity team, working for Alibaba, who disclosed it to the developers so a patch could be released.

However, by not first reporting the vulnerability to the CCP, Alibaba ran afoul of a recently passed law called the "Provisions on Security Loopholes of Network Products", which requires all Chinese companies to report vulnerabilities to the CCP. Alibaba's security team was publicly and harshly reprimanded and removed from the prestigious Chinese Ministry of Industry and Information Technology for at least 6 months[12].

Reporting vulnerabilities to vendors is a cybersecurity industry norm. However, if nation-states begin to encourage or enforce disclosure to parties interested in ensuring vulnerabilities remain unpatched, it could have ramifications for every business. As fewer vulnerabilities being reported to vendors for patching will leave the door open for cybercriminals.

[10] https://www.cpomagazine.com/cyber-security/as-ukraine-war-rages-conti-ransomware-gang-throws-support-behind-russian-government/
[11] https://blog.malwarebytes.com/threat-intelligence/2022/03/the-conti-ransomware-leaks/
[12] https://www.wsj.com/articles/china-halts-alibaba-cybersecurity-cooperation-for-slow-reporting-of-threat-state-media-says-11640184511

Conclusion

Given the extremely low likelihood of a nation-state actor launching a direct, targeted attack against an Australian SME, and the significant investment required to fend off such an attack, very few should be concerned with the direct risk posed by nation state actors.

However, a worrying large amount of global cybersecurity issues can be traced back to the actions of nation-state actors as they attempt to covertly support their nations policy, or as their cyberweapons are released, lost control of, or leaked.

With the current escalating global tensions, there is an increasing risk that sophisticated cyberweapons will be released and the repurposed by criminal elements, and an increasing risk of Australian SMEs become collateral damage in a larger cyberconflict.

Fortunately, these risks are similar to those already faced and known, and the defence techniques are the same. SMEs with existing strong cybersecurity practices only need to increase their vigilance, as baseline security controls aligned to frameworks such as the Essential 8 or NIST continue to provide cost effective risk mitigation for SMEs even in the current global climate.

advance

Contact Info

● +61 8 8238 6500

● sales@advance.net.au

● www.advance.net.au